UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/456,794	12/08/1999	JAY C. CHEN	34581/CAG/C718	6924

7590 07/14/2005

McDermott Will & Emery
Attn: Craig A. Gelfound
2049 Century Park East
34th FL
Los Angeles, CA 90067-3208

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/456,794	CHEN, JAY C.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *82-116* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *82-116* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 82-116 remain pending and have been examined.

Response to Arguments

2. Applicant's arguments with respect to claims 82-116 have been considered but are not persuasive.

The Applicant asserts that there is no desirability to the combination of Ginzboog with the Woo-Lam protocol as taught by Schneier. The applicant asserts that the desire to verify a digital signature in Ginzboog would not motivate one of ordinary skill in the art to utilize the Woo-Lam protocol. Yet Ginzboog clearly discusses the desirability of signature verification at the passage cited. The applicant asserts that since Ginzboog teaches an alternate form of signature verification there would be no motive to incorporate Woo-Lam and EKE as taught by Schneier. Yet Ginzboog points to a motive for his invention as: "It is because of the aforementioned reasons that studies are under way to determine the possibility of using the ordinary subscriber line (twisted pair cable) for high-speed data transmission, in other words, for speeds that clearly exceed the speed of the ISDN basic connection (144 kbit/s). The present ADSL (Asymmetrical Digital Subscriber Line) and HDSL (High bit rate Digital Subscriber Line) technologies offer new possibilities for high-speed data and video transmission via the telephone line to subscriber terminals." (col. 1 lines 35-40). Use of Woo-Lam and EKE would offer the advantage of higher speed as the majority of transaction processing would take place at the subscriber. The mere recitation of the applicant's preferred embodiment in

Ginzboog does not automatically imply that such is the best approach, only that it is the one selected by Ginzboog.

The Applicant asserts that the Walker reference does not teach the sending of a key. Yet such was not asserted by the Examiner in the rejections of the claims. It is unclear which claim rejection the Applicant is attempting to traverse with this argument.

The applicant asserts that the key exchange request generated by a member using the Woo-Lam protocol does not include the member's public key. Yet the fact that Trent may send Bob Alice's public key in step 5 indicates that such a key exchange between Alice and Trent occurs in Woo-Lam.

The Applicant asserts that: "It is improper... to rely on Encrypted Key exchange protocol for the concept of generating a session key exclusively at the service provider." The applicant asserts that this is improper because Woo-Lam and Ginzboog do not teach establishment of a shared secret. Yet the exchange of random numbers in Woo-Lam constitutes such.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 82-84, 86, 88-90, 92-94, 96, 97, 103, 104, and 106-116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboog US 6,240,091, in View of Schneier, Applied Cryptography 2nd Edition, Oct. 1995.

As for claim 82, Ginzboog teaches a method of conducting an electronic transaction using an electronic card having a public key of a service provider comprising (abstract, fig. 3a, col. 7 lines 51-67); Schneier teaches the features of the claim not taught by Ginzboog, namely formatting a key exchange request message at a member (page 64: Woo-Lam step 3), the key exchange request message having a public key of the member, and at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card (page 64: Woo-Lam step 3): sending the key exchange request message from the member to the service provider (page 64: Woo-Lam step 3): generating a session key at the service provider in response to the key exchange request message (page 64: Woo-Lam step 5): formatting a key exchange response message including the session key at the service provider; sending the key exchange response message from the service provider to the member (page 64: Woo-Lam step 5), and using the session key to complete the transaction (page 64: Woo-Lam steps 6-8). Schneier teaches a two party public key based key exchange protocol where one participant in the exchange is exclusively tasked with generating a session key (page 518: EKE protocol step 2). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these steps into the method of Ginzboog. Motive to make this combination

is found, for example, in col. 3 line 60 through col. 4 line 2 of Ginzboog where the desirability of signature verification of subscriber access is discussed. The Woo-Lam and EKE key exchange protocols are public key based and therefore allow verification by well-known public key techniques of digital signatures.

As for claim 83, Schneier teaches the steps of the claim not taught by Ginzboog, namely a method of wherein the key exchange request message further includes a member challenge for the service provider (page 64: Woo-Lam step 4), and the key exchange response message further includes a response to the member challenge and a service provider challenge for the member, the method further comprising formatting by the member a response to the service provider challenge and sending it to the service provider (page 64: Woo-Lam step 5). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these steps into the method of Ginzboog. Motive to make this combination is found, for example, in col. 3 line 60 through col. 4 line 2 of Ginzboog where the desirability of signature verification of subscriber access is discussed. The Woo-Lam and EKE key exchange protocols are public key based and therefore allow verification by well-known public key techniques of digital signatures.

As for claim 84, Schneier teaches the steps of the claim not taught by Ginzboog, namely a method wherein the use of the session key to complete the transaction comprises: formatting by the member a transaction request message using the session

key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member (page 64: Woo-Lam steps 6-8). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these steps into the method of Ginzboog. Motive to make this combination is found, for example, in col. 3 line60 through col. 4 line 2 of Ginzboog where the desirability of signature verification of subscriber access is discussed. The Woo-Lam and EKE key exchange protocols are public key based and therefore allow verification by well-known public key techniques of digital signatures.

As for claims 86, 90, 94, and 97 Schneier teaches the steps that Ginzboog fails to teach, namely a method wherein the transaction request or response message comprises plain text (page 64: Woo-Lam step 1). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this step into the system of Ginzboog. It would have been desirable to do so as this would decrease to computational overhead for the subscriber initiating the transaction.

As for claim 88, Schneier teaches the method step that Ginzboog fails to teach, namely that the transaction request message comprises the response to the service provider challenge (page 64: Woo-Lam step 3). Therefore it would have been obvious to

one of ordinary skill in the art at the time of the invention to incorporate this step of Schneier into the system of Ginzboog. It would have been desirable to do so as this would allow for authentication of a subscriber prior to initiation of a request.

As for claims 89 and 93, Schneier teaches the method steps that Ginzboog fails to teach, namely wherein the transaction or acknowledgement response message includes data encrypted with the session key (page 518 EKE step 2, 4). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this step of Schneier into the system of Ginzboog. It would have been desirable to do so as this would allow for increased security in responding to a subscriber request.

As for claims 92 and 110, Schneier teaches the features of the claim not taught by Ginzboog, namely a method further comprising formatting at the member, using the session key, a transaction acknowledgment message, digitally signing by the member the transaction acknowledgment message, and sending the transaction acknowledgment message to the service provider (page 51: Key and Message Transmission steps 1-6). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this step of Schneier into the system of Ginzboog. It would have been desirable to do so as this would allow for increased security in responding to a transaction acknowledgment.

As for claim 96, Ginzboog teaches a method of conducting an electronic transaction using an electronic card having a public key of a service provider (abstract, fig.3a, col. 7 lines 51-57). Schneier teaches the features of the claim not taught by Ginzboog, namely generating a member challenge by a member; encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram (page 64: Woo-Lam step 4); formatting by the member a key exchange request message including the first cryptogram and a public key of the member; signing digitally by the member the key exchange request message; sending the digitally signed key exchange request message from the member to the service provider (page 64: Woo-Lam step 4, page 518: EKE step 1); generating by the service provider a service provider challenge (page 518: EKE step 4); generating exclusively by the service provider a session key; encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram (page 518: EKE steps 3-5); formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge; signing digitally by the service provider the key exchange response message; sending the digitally signed key exchange response message to the member; encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram (page 518: EKE steps 3-5); attaching the third cryptogram to a transaction message going from the member to the service provider; signing digitally by the member the transaction

message going from the member to the service provider; and sending the transaction message from the member to the service provider (page 518: EKE steps 5, 6).

As for claims 103, 106, 111 and 113, Schneier teaches the features of the claim that are not found in common with claim 82 above and as taught by the combination of Ginzboog and Schneier as applied to that claim, namely sending the first key exchange request message from the first member to a second member; combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider and where the first and second session keys differ (page 59: Otway-Rees steps 1 ,2) Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this step of Schneier into the system of Ginzboog. It would have been desirable to utilize this first communication step between a first and a second member in order to prevent replay attacks.

As for claims 104, 114 and 115, Schneier teaches the features of the claim not taught by Ginzboog, namely formatting by the first member, using the first session key, a transaction request message, signing the transaction request message, and sending the transaction request message to the second member (page 59: Otway-Rees step 1); formatting by the second member, using the second session key, a transaction request message where the first and second session keys differ form one another; combining by

the second member, the second member transaction request message with the first member transaction request message, signing the combined transaction request message, and sending the combined transaction request message to the service provider (page 59, Otway-Rees step 2); formatting by the service provider, using the first session key, a transaction response message for the first member, and signing the transaction response message; formatting by the service provider, using the second session key, a transaction response message for the second member (page 60, Otway Rees step 3); combining the transaction response message for the first member with the transaction response message for the second member to form a combined transaction response message, and signing the combined transaction response message, sending the combined transaction response message to the second member (page 60: Otway-Rees step 3); separating at the second member, the transaction response message for the first member from the transaction response message for the second member; and forwarding by the second member the transaction response message for the first member to the first member (page 60: Otway-Rees step 4). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this step of Schneier into the system of Ginzboog. It would have been desirable to utilize this first communication step between a first and a second member in order to prevent replay attacks.

As for claims 107, 112 and 116, Schneier teaches the features of the claim not taught by Ginzboog, namely a first session key that is the same as the second session

key (page 64, Woo-Lam step 4). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Schneier into the method of Ginzboog. It would have been desirable to do so as this would speed communications via the use of a symmetric protocol.

As for claim 108, Schneier teaches the features of the claim not taught by Ginzboog, namely that the key exchange response message for the second member includes the public key of the first member, and the key exchange response message for the first member includes the public key of the second member (page 64: Woo-Lam steps 1-6). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Schneier into the method of Ginzboog. It would have been desirable to do so as this would speed communications.

As for claim 109, Schneier teaches the features of the claim not found in common with claim 82 and taught by the combination of Ginzboog and Schneier, namely sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member (page 64, Woo-Lam steps 1-6). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Schneier into the system of Ginzboog. It would have been

desirable to do so as this would allow for the use of a centralized key distribution center in group or multicast message processing.

5. Claims 85 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboog and Schneier as applied to claim 82 above, and further in view of Walker, US 6,263,438.

As for claim 85, the combination of Ginzboog and Schneier does not teach a transaction request message that includes account information, transaction amount and transaction data, and wherein the formatting of the transaction request message by the member comprises encrypting with the session key the account information, the transaction amount and a portion of the transaction data. However, Walker et al. does teach the encryption of financial transaction data by a such a symmetric key (col. 1 lines 20-23, col. 4 lines 5-10). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these steps into the system of Ginzboog and Schneier. It would have been desirable to do so as this would increase the utility and hence marketability of the system.

6. Claims 87, 91, 95, 98-102, and 105 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboog and Schneier as applied to claim 84 above, and further in view of Official Notice.

As for claims 87, 91, 95, 100-102, the combination of Schneier and Ginzboog fails to teach a method wherein the transaction request, response or acknowledgement message comprises a transaction identification assigned to the member by the service provider. However Official Notice may be taken that the use of such subscriber identifiers is a step that is old and well known in the art of secure financial network communications such as ATM networks utilizing a customer PIN during transaction initiation from remote terminals. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these steps into the system of Ginzboog and Schneier. It would have been desirable to do so as this would increase the utility and hence marketability of the system.

As for claim 98, the combination of Ginzboog and Schneier fail to teach a step wherein the key exchange request message comprises the member's public key encrypted with the service provider's public key. However Official Notice may be taken that such a key request message is old and well known in the art. Such a key request message is commonly used in requests made of public key certificate authorities. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this step into the method of Ginzboog and Schneier. It would have been desirable to do so as a key request signed in this manner would allow for increased security in key transmission.

As for claims 99 and 105, Schneier teaches the features of the claim not taught by Ginzboog, namely formatting at the first member, using the first session key, an

acknowledgment message, signing the acknowledgment message, and sending the acknowledgment message to a second member (page 60: Otway-Rees step 4); However the combination of Schneier and Ginzboog fails to teach the step of formatting at the second member, using the second session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message to form a combined acknowledgment message, signing the combined acknowledgment message, and sending the combined acknowledgment message to the service provider. However Official Notice may be taken that such a step of using a combined acknowledgement message is old and well known in the art. Multicast key exchange protocols commonly use such combined acknowledgement messages from a node to a key broadcast center where the message is a combined acknowledgement. It would have been desirable to incorporate this step into the method of Ginzboog and Schneier as this would help to foil any attempted replay attacks.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chen 5,784,463

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

7-11-2005

Paul Callahan